Exploring Website Location as a Security Indicator

Der-Yeuan Yu, Elizabeth Stobert, David Basin, Srdjan Capkun
Department of Computer Science, ETH Zurich

ABSTRACT

Authenticating websites is an ongoing problem for users. Recent proposals have suggested strengthening current server authentication methods by incorporating website location as an additional authentication factor. In this work, we explore how location information affects users' decision-making for security and privacy. We conducted a series of qualitative interviews to learn how users relate location to their online security, and we designed a security indicator to alert the user to changes in website locations. We evaluated our tool in a 44-participant user study and found that users were less likely to perform security-sensitive tasks when alerted to location changes. Our results suggest that website location can be used as an effective indicator for users' security awareness.

ACM Classification Keywords

H.5.2 Information Interfaces and Presentation (e.g. HCI): User Interfaces; K.6.5 Management of Computing and Information Systems: Security and Protection

Author Keywords

Website location; security indicators; user study.

INTRODUCTION

The Internet is a central medium for global information exchange. Users' reliance on the Internet for critical services, such as banking, data storage and communication, highlights the importance of data security. However, there is no way for users to know whether their privacy is respected. For example, it is often unclear whether online firms reveal users' profiles to third parties, such as advertising firms or government agencies. The risk of personal data leakage requires users to determine, consciously or subconsciously, whether a website is trustworthy enough. This is an extra burden on users since security is not usually their primary goal [43].

Users' trust in websites is strongly tied with the problem of server authentication, currently achieved using public key certificates. Browsers typically display a green lock icon to indicate successful authentication or a warning otherwise. Research has found that users frequently ignore or bypass related warnings, making themselves vulnerable to online threats [3, 4, 38]. Users also often fail to notice or comprehend certificate information [14, 37], which has been addressed with improved interface design [15, 16, 36, 39]. As website impersonation attacks increase, there have been new approaches to strengthen server authentication. One direction of research proposes using the server's geographic location as an additional trust factor [1,44]. However, the usefulness of such information depends critically on how it is presented to users and how they in turn perceive and evaluate it. Until now, these questions have been unexplored.

In this paper, we explore users' decision-making processes regarding their security and how website locations can play a role. Using a user-centered design approach, we gathered requirements, designed a location indicator, and evaluated its usability. We conducted semi-structured interviews with 15 participants and applied thematic analysis to identify factors relevant to online trust and the significance of website locations in their decisions. We found that participants expressed preferences for particular locations when dealing with sensitive information or transactions. This suggests the potential for leveraging location information as a new trust factor.

Based on the interview results, we defined requirements for a location tool to inform users of website locations. We implemented LocationWatch, a Chrome extension that makes users aware of website locations and alerts them to changes in server locations. Using LocationWatch, we conducted a user study with 44 participants to analyze how website locations affect their decision-making processes. Our statistical analysis showed that participants' decisions were significantly affected by website locations, with fewer users completing sensitive tasks when the website location had changed. Participants' decisions also varied depending on the sensitivity of data in different scenarios.

The effects of website location knowledge have not been investigated until now in the literature. With recent proposals for strengthening authentication using website locations, it is important to evaluate how this information is perceived by users and how it can be best leveraged in their decision-making processes. Our results show that users are sensitive to website locations when informed in a non-intrusive way. This shows the promise of using location information as an additional security factor.

BACKGROUND

Current research on location-based website authentication raises the question of how users might leverage such location information in decision-making. Compared to digital certificates, the tangibility of location and its clear relationship to the real world suggests that location can play a role in users' security and privacy awareness.

Location-based Decision-Making

Psychological research on decision-making has found that people tend to underestimate risk. Since safety

and security are abstract concepts, users are unmotivated to pay attention to these risks. Research examining how users make decisions about computer security has found that users reason inconsistently about their gains and losses, and are likely to overprioritize the cost of losses [42]. For security, because the gains are abstract and the consequences seem random, users often focus on costs, which are immediate and tangible [42]. Hardee, West, and Mayhorn [22] found that users consider gains, such as protecting information, money, and property, but that they are unaware of risks relating to money and property loss online. Users are also concerned about personal inconvenience in using online services.

Users' security decisions often serve to protect their personal privacy. Research has found that users' privacy preferences are context-dependent and easily influenced [2]. Users also experience high uncertainty about whether and to what extent they should be concerned about data privacy. Human decision-making can appear inconsistent, but it is governed by a complex calculus of decision-making [29] that factors in additional information such as social norms and emotional responses.

Although other researchers have explored location and privacy for users [8, 12, 23], most existing research has been in the context of having the user share their own location with online services or other parties. Fisher et al. [17] studied iPhone users and found that they used permissions-based access control to limit their location-sharing to certain applications. Patil et al. [32] found that while users were motivated to share their locations for social purposes and in-app rewards, they overwhelmingly desired location-sharing to be explicit. While our work addresses an opposing issue, this research emphasizes the importance of location as a relevant factor in security and privacy decisions.

Little research to date has analyzed users' perceptions of where their data is stored or to what locations it is transmitted over the Internet. Kang et al. [28] conducted a qualitative study investigating users' mental models of the Internet and found that users had only a vague understanding of where data is stored online. They also found that factors such as reputation and appearance were likely to influence users' perceptions of what was happening to their data. Ion et al. [24] interviewed users about their data privacy awareness and their attitudes about where their online data should be kept. They found that users generally preferred sensitive data to be stored locally than uploaded to cloud storage. They also identified cultural differences that affect users' understanding and preference for their online privacy. A large-scale study of website credibility [18] found that websites were more believable when they communicated the "real world" aspect of the organization, were professional and easy to use, and included indicators of trustworthiness. It remains unexplored how users might integrate information about the website's location into their evaluation of these environmental cues.

Website Location and Authentication

Recent work has proposed using location as an authentication factor for web servers, relying on the precision and uniqueness of private website locations. Yu et al. explored the use of location in addition to digital certificates to authenticate servers in TLS handshakes [44]. This approach requires a trusted party to estimate the location of a website server and issue a signed statement binding the server location to a particular connection with the client. The browser can either perform automatic verification (e.g., during the TLS handshake) of the location information or directly display it to the end user. Abdou and van Oorschot proposed similar methods of augmenting TLS by actively estimating website locations using delay-based measurements from multiple locations [1]. Both works propose the concept of integrating website location into server authentication and the use of pinning techniques to detect location changes.

This use of location as an authentication factor is increasingly possible due to the availability of pervasive location information, IP geolocation services, and general localization techniques. A non-technical approach to website localization is the use of public ledgers to record and make available the location of data centers. Online services often host their website servers in data centers, whose locations are accessible in the public domain. For example, online resources such as Data Center Knowledge [33] provide a public listing of data center deployment and news about web hosting companies. Companies are increasingly disclosing their server locations to the public [5, 20], and using on-site security to protect critical online services from physical intrusion by malicious parties [21, 40]. In addition to out-of-band channels, website locations can also be encoded in Extended Validation (EV) certificates [11] as part of the Subject field, which can be extracted by the browser.

Commercial IP geolocation solutions, e.g., MaxMind [30], Geobytes [19], IP2Location [25], and IPligence [26], allow users to query for accurate website locations using IP addresses. These services use public WHOIS databases maintained by regional Internet registrars (such as ARIN [7], RIPE [34], and APNIC [6]). The accuracy of IP geolocation is further improved using a wide range of sources, such as user-submitted data or detailed information provided by the local ISP. Currently, IP geolocation is the most common source of website location data. There also already exist software solutions showing IP geolocation data to users, such as Flagfox [13] and IP Whois & Flags [31]. These solutions support other features such as site safety checks and ratings, but their impact on users' security awareness and decisions has not been explored in depth.

RESEARCH OVERVIEW

Given the increasing availability of server location information[1], our goal was to explore how it is or can be

[1]To make it easier for the user study participants to understand, we used the term "website locations" in our user

leveraged as part of users' trust in websites and online services. More specifically, we aimed to answer the following research questions.

Q1 How do users currently make online security decisions and how does website location play a role?
Q2 Does the information about website locations affect users' behavior?

We explored these problems using a user-centered design approach [27]. To answer Q1, we conducted a series of qualitative interviews and applied thematic analysis to understand users' decision-making processes for online security. The themes we identified allowed us to develop design requirements for a website location interface for a broad range of web users. To answer Q2, we designed a location indicator that displays the website's location. The indicator is implemented and incorporated into Chrome as an extension. Finally, we conducted a user study to evaluate the usability of our interface and analyze the impact of location knowledge on users' decisions in real-world application settings. All studies involving human subjects were approved by our institution's ethics committee.

STUDY 1: USER INTERVIEWS

We first interviewed users about how they currently determine websites' trustworthiness and how server locations play a role. Our goal was to identify factors that could lead to the development of design requirements for a location indicator.

Study Design

We chose a semi-structured interview approach to ensure that we covered topics of interest while giving participants the freedom to discuss their decision-making processes and concerns. Our interview covered three areas: Internet use, location and security awareness, and location-related preferences. We carefully selected topics that might have associated security or privacy concerns for different Internet usage scenarios: online file storage, emails and calendars, online financial transactions (banking and shopping), and social media. For each topic, we asked how participants used these services, what kinds of data they stored or obtained through those services, and what kinds of security and privacy concerns they had around these activities. Regarding location and security awareness, we asked participants about their general security and privacy precautions and where they thought Internet data was stored and served from. Because we were interested in the development of a security indicator, we asked about how they currently determine that websites are legitimate or trustworthy. Finally, we asked participants how they might use available location information in their decision processes.

In our interview design, we made an effort to encourage discussion on a wide range of topics with relevant security and privacy concerns. Rather than specifically introducing technical concepts related to location-based authentication, we introduced topics that naturally led to the subject of location. If participants did not bring up the subject of location on their own, we attempted to steer the conversation in that direction. We audio-recorded the interviews to facilitate subsequent note-taking and transcription for analysis. Participants also filled in a demographics questionnaire before the interview. Each interview lasted between 30 and 60 minutes.

studies. We use the terms "website locations" and "server locations" interchangeably throughout the rest of the paper.

Participants

We recruited people of different genders, ages, education levels, occupations, and diverse nationalities. We deliberately advertised outside our institution using public bulletin boards, online forums, and mailing lists. While our sample is likely not representative of the larger population, we feel confident that a variety of viewpoints were expressed in our interviews, and that the perspectives and experiences expressed were in line with the results of similar studies [17, 28].

We reached saturation at 15 participants (8 female, 7 male). They ranged in age from 20 to 59, with most aged between 20 and 39 years old (13 participants). Participants' nationalities spanned 12 countries. They had a variety of educational backgrounds, and their areas of study included social and natural sciences, engineering/informatics, and healthcare. Their occupations included artists, scientists, and students. To provide a rough measure of the participants' level of international experience, we asked participants how many countries they had visited. The participants had visited a median of 10 countries.

Thematic Analysis

Following completion of the interviews, we reviewed the audio recordings and transcribed each interview. This produced a qualitative dataset that we analyzed using thematic analysis [9], a flexible qualitative analysis methodology that allowed us to identify themes and relationships in the data. We began our analysis with open coding. We traversed and reviewed the transcriptions line by line and assigned codes to recurring ideas. To ensure consistency, each interview was coded by two researchers, and codes were cross-checked for reliability.

As an example, when asked about how she verified website authenticity, a participant replied:

> "Actually I didn't think of [authenticating websites] before. I think every website will give us some legal documents to read before we give information to them. I will scan the documents." – P5

We assigned the code *lack of awareness* to highlight her lack of concern. Because she mentioned her attention to legal documents, we assigned the code *legal concern*. We identified 46 open codes in our data. We refined the codes and classified them into themes, described below.

These themes highlight patterns of typical behaviors we observed, rather than representing categories of users.

Inherent Trust

Many participants took the security of websites for granted and asserted that online services were trustworthy without much investigation.

> "Well, I mean, [website authentication] is not something I think about. You just go to the webpage, it looks familiar, and then it never crosses your mind that it may have been forged." – P12

We also noticed users' inherent trust from the way they described their automatic use of various online services, such as synchronization of data (e.g., contacts and files) across different devices linked to the same platform.

> "I think I do use sometimes iCloud. I think it just come automatically with my iPhone. Each two weeks, asking me if I want to store it [...] I think mainly I, I just let it." – P1

Most participants embraced the convenience of automated functions, such as allowing web email servers to automatically store email addresses of frequent contacts, and took their trustworthiness for granted.

Overall, many participants appeared to have a default passive approach towards online security, which was to trust the way things were. They did not frequently engage in discussions of security and privacy until faced with potential online risks or sensitive applications such as banking and shopping.

Diverse Trust Concerns

While a few described themselves as generally indifferent, most participants had numerous concerns regarding the security and privacy of their data. These included worries about their personal privacy, financial safety, and freedom of speech.

Personal privacy was a major concern that was repeatedly brought up during the interviews. Participants discussed privacy concerns about sharing information with both online services and other users of those services.

> "I just kind of like the idea of not being very traceable, not because I'm hiding something specifically but because it's my own business kind of, where I am, what people I'm seeing." – P14

Some participants were aware of data collection by corporations, but had decided to ignore the implications, or did not perceive this as a threat.

> "I don't really see the problem. I mean, okay, [online services] are going to have my numbers, and other numbers, but it doesn't really affect me." – P2

However, some participants acknowledged the need for personal information disclosure. For example, for public security, P5 stated that "sometimes we have to be checked by other people." Others mentioned the used of their public profile information for professional networking. Many regarded the purpose of the Internet as being to share information and said that curtailing this sharing renders their online presence less meaningful.

Financial security was a major concern, and many participants discussed security concerns around online banking and shopping. Participants were also concerned about the future consequences of sharing information and opinions online.

> "I don't really trust that [my words] might not one day be used against me... I think a lot of this information is stored and it's just uncomfortable." – P14

Multiple Trust Factors

Participants mentioned a variety of factors that encouraged them to trust websites. While a few participants were aware of security indicators such as certificate validation, most participants associated website trustworthiness with impressions, such as familiarity of brand presentation and the website interface. Even knowledgeable participants admitted to relying on such visual cues.

> "I think the first [thing I notice] would be the brand, the logo itself [...] does it look the same?" – P2

Participants also relied on experience from peers or website reviews to judge whether websites were trustworthy.

> "[How do you choose where to shop online?] ... usually based on the community. [...] I always try to think or to ask friends if they have ever bought something in that website." – P10

One major trust factor was the reputation of the company. For example, when asked about why they trust particular storage services, some participants relied on the brand name: "... I think having the Apple's name behind it, it's quite safe." (P3) Participants also listed companies such as Google and Amazon as their trusted service provider. Many preferred to avoid unknown third-party shopping websites and rely on payment services with buyer protection policies (e.g., PayPal).

Decision-Making Process

Most participants described clear heuristics for online decision making based on their trust factors and concerns. These included using pseudonyms, providing fake profile information, avoiding saving credit card information on websites, and only buying from familiar vendors.

However, participants often admitted to bending their rules or making exceptions for practical reasons. They often justified these decisions by discussing the acceptability or manageability of the potential risks, e.g., a small financial risk when ordering from an untrustworthy merchant. Participants also frequently indicated that their decisions depended on the urgency of the matter at hand. They put themselves in insecure situations (such as by ignoring the website certificate warnings) to ensure convenience and access to online services. In such situations, participants often described a tradeoff

between personal security and service accessibility when making their decisions. Though security compromises were made, participants mentioned various secondary measures to reinforce their decisions, such as obtaining tangible proofs of their transactions (e.g., confirmation printouts) or contacting customer service.

Helplessness

During the discussion of their decision-making processes and concerns, participants often expressed frustration over missing information or knowledge. Many expressed helplessness relating to their inability to understand security measures, and their lack of control over corporate policy, such as where user data is stored.

> "[How do you know you are visiting the real website?] I don't think too much on these things because I don't know exactly how it works." – P1

Participants also acknowledged the burden of responsibility accompanied by additional information. As a result, some participants felt that security obligations were being delegated to them.

> "If location would be available for me, I would have a feeling that from that time I am the one who has to be responsible for that also." – P7

Location Awareness

Unsurprisingly, participants had generally not considered issues relating to location and Internet security. They were unaware of the geographic locations of web servers and where their data was stored. Several participants speculated that data must be stored in the same countries where the parent companies were based.

Although many participants were unable to envision exactly how they would leverage verified location information to establish trust, they were able to articulate ways in which location already influences their trust decisions. Some participants expressed clear preferences for certain countries or regions due to their reputable privacy regulations and law enforcement (mainly in the context of financial transactions).

> "I would say it is important to be sure they are stored in countries with high security levels... I would say in the first place legal regulations: who is allowed to have access and under what conditions someone could have access to such data. And in Europe, I would say such [legal institutions] are on a high standard." – P11

Participants also referred to public disclosures of nation level surveillance programs (e.g., mass surveillance in the USA) and other data-gathering concerns when discussing where they avoid sharing or storing data.

Participants generally thought location information could be most helpful for sensitive applications such as banking. A participant also identified the potential of location being incorporated into security mechanisms.

> "But I think in the end it will be used everywhere because it would be like a, like an adapted protocol. I think for me it would be useful into banking, into this kind of banking scenarios..." – P4

Summary

The participants varied considerably in how they made trust decisions. They mostly trusted websites and online services based on the impression of their reputation. When discussing online activities, participants cited financial security and personal privacy as their primary security concerns. Their decision-making processes for determining website trustworthiness were composed of typical security practices and pragmatic workarounds when the associated risks were deemed acceptable.

Our analysis revealed that website locations, although not often directly acknowledged by participants, played a role in their online decisions. When discussing trust factors, we found that participants were more receptive to discussions of website locations as opposed to traditional security solutions, such as public key certificates or authentication. This showed that there is a gap between the desired goals of current security indicators and their effects on users' decision making. It also suggested the potential of using website location to improve user security awareness and decision making. To evaluate users' perception of and response to such information, we required an assistive tool to display website locations.

DESIGN OF OUR LOCATION TOOL (LocationWatch)

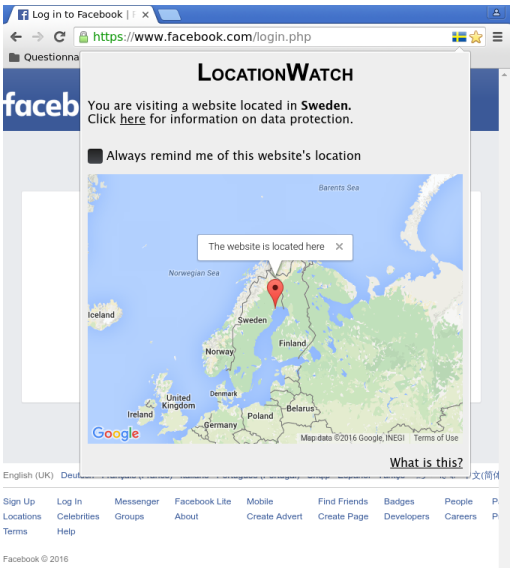
Based on our qualitative analysis, we developed a set of design requirements for our location tool, LocationWatch. We implemented LocationWatch as a Chrome extension featuring: a flag indicator, a location tip, and a warning message. The flag indicator (Figure 1a) is an icon near near the address bar showing the flag of the server's residing country. The location tip (Figure 1b) is a small window on the upper-right side of the window that appears on the first visit to a website. The warning message (Figure 1c) appears when a website's location has changed. The locations can be obtained using upcoming website localization techniques [1,44]. Since these methods are still under development, LocationWatch uses IP geolocation databases as a reference.

Design Requirements

We aimed to implement LocationWatch as an easy-to-use, unobtrusive, and effective tool to display website locations. For each theme from our qualitative analysis, we identify their implications on our design choices.

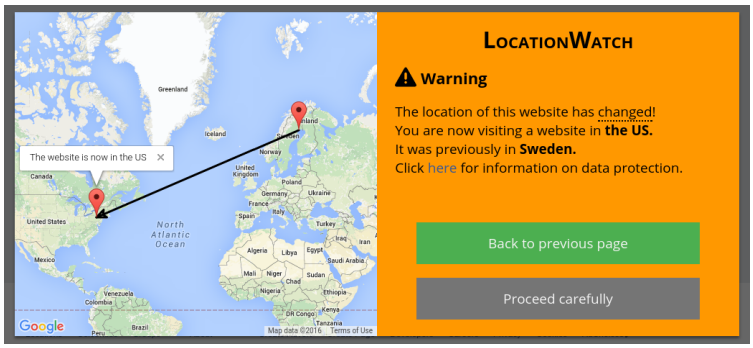
Inherent Trust

Participants often said they trusted online services by default and neglected to pay attention to security indicators. This shows a need to make security information intuitive for the users. Some may also prefer not to be bothered with location details since website security is not their primary task. We therefore designed LocationWatch to be non-intrusive by showing only the flag icon by default so that it does not disturb uninterested users.



(a) The flag indicator and popup.

(b) The location tip shown on the initial visit to a website.



(c) The warning when a website's location has changed

Figure 1: Features of LocationWatch, our location indicator.

Diverse Trust Concerns

Participants were generally concerned about how their private data was used or misused. Since legal protection laws differ across countries, the location of where data is stored or sent may prompt different user concerns and influence subsequent decision-making. We designed a popup (Figure 1a) that appears when the user clicks on the flag icon. This popup shows the server's governing country, and information on that country's data protection laws for the users' reference. The location tip acts as a visible notification for the user on the first visit. The user can also opt-in to see this tip for every visit.

Multiple Trust Factors

Many participants considered the visual familiarity of websites as a primary factor for trust. Although webpage presentation does not imply server authenticity, a change in what the user sees may trigger security awareness or suspicion. We therefore use visual cues to notify users. First, the location tip appears on the user's initial visit to a website (Figure 1b). Users are also visually informed when the website's location has changed. This is realized using the warning message (Figure 1c) which displays the current and previous website locations.

Decision-Making Actions

Participants mentioned making exceptions for practical reasons, often due to a personally-established acceptable level of risk. Our location indicator does not prohibit such choices, as is available with certificate warnings. In the warning message, we provided two buttons: "leave the website" and "proceed carefully" (Figure 1c). The phrasing of these buttons were aimed to hint that users should reconsider the security of their decisions.

Helplessness

Participants were often frustrated with technical security measures due to their lack of knowledge and control. The location indicator should have obvious signs, simple and intuitive explanations, and clear actions for the user to take. As a result, LocationWatch contains only simple textual information with a link to detailed legal reference. Users can control when the warning message is shown, allowing them to decide whether and to what extent to consider location information.

Location Awareness

Participants often expressed preferences for certain countries to store their data. This also suggested that country information is a suitable level of detail for the indicator to show to most users. Since some users may want more information about data center locations, detailed locations should also be available. We support this by showing the detailed location using a map in the popup window (Figure 1a).

STUDY 2: USER EVALUATION

To evaluate the impact of the information provided by LocationWatch on users' decision-making processes, we conducted a user study. First, we aimed to evaluate the usability of our location interface to see if it satisfied our design concepts and requirements. Positive user feedback would suggest the potential of location as useful added information for users. Second, we aimed to evaluate how users' security awareness in online services changes when website locations are provided. In the qualitative analysis, we found that many users relied on past experiences and impressions of the website. We

Stage	Tasks	Location	Ctrl features	Expt features
1	Dropbox: upload passport scan	United States	Flag	Flag + Tip
Initial Visit	Facebook: update status	Sweden	Flag	Flag + Tip
	Banking: check 1st account balance	Switzerland	Flag	Flag + Tip
2	Dropbox: upload password list	United States	Flag	Flag (+ Tip)*
Re-visit	Facebook: update status	Sweden	Flag	Flag (+ Tip)*
without change	Banking: check 2nd account balance	Switzerland	Flag	Flag (+ Tip)*
3	Dropbox: upload credit card	China	Flag	Flag + Warning
Re-visit	Facebook: upload party photo	United States	Flag	Flag + Warning
with change	Banking: check 3rd account balance	Japan	Flag	Flag + Warning

*The tip is only shown if the participant checked the "always remind me" option in Stage 1.

Table 1: Study 2 tasks and location configuration for the control and experiment groups.

therefore hypothesized that website location changes between subsequent visits would alarm users and could be used as an indicator of their security awareness.

Study Design

To evaluate LocationWatch and users' response to website locations, we designed an experiment where participants used three web services (file storage, social networking, and online banking) and performed routine but potentially sensitive tasks. We chose these services to prompt typical concerns from the qualitative analysis: personal privacy, identity safety, and financial security. We aimed to measure how online behavior varied when participants were given website location information using LocationWatch.

Our study had a mixed design, where condition was a between-subjects factor and stage was a within-subjects factor. There were two conditions: control and experiment. In the control condition, the location interface was configured to show only the flag icon and the popup window (making it similar to existing tools [13, 31]). In the experiment condition, participants used the fully-featured version of LocationWatch, including the location tip and the location change warning. The study had three stages and in each stage the participant was asked to perform three tasks, as shown in Table 1. We used a Latin square design to shuffle the task order across different participants in each stage to avoid order effects.

Each participant was given a brief introduction to the study's purpose as a usability evaluation of a software tool. All participants received the same tutorial on LocationWatch, introducing the concept of geographic locations of websites, the flag icon, and the popup features. To avoid priming users to expect location changes, we did not reveal the location tip and warning (these features were only available to the experiment group). Participants were then given login information for the accounts and files created for the studies and instructed to treat them as if they were their own.

We chose to have the interface show three types of locations: neutral countries typically associated with good privacy impressions (Sweden, Switzerland, Japan), a developed country with widely-reported data privacy breaches (the USA), and a developing country with known Internet censorship (China). We also chose plausible locations for the services used in the study. For the last stage of the study, we programmed LocationWatch to show location changes: Dropbox to China, Facebook to the USA, and the online bank to Japan. For the control group, this resulted in a change of the country flag and contents in the popup. For the experiment group, the location change warnings were additionally shown.

Each session lasted between 30 and 60 minutes, and the study was conducted in our lab to facilitate observation and discussion. In addition to instrumented data collection about their interaction with the tool, participants also completed three questionnaires during the study: demographics, a pre-test questionnaire about their online decision-making habits, and a post-test questionnaire about their impressions of the usability and security of LocationWatch.

Participants

We recruited users who were aged 18 years or above, spoke English, and had experience browsing online, including experience with online banking. 44 participants completed the study (23 female and 21 male), most of whom were students (32). They ranged in age from 20 to 59, with most (34) being between 20 and 29 years old. Participants' nationalities spanned 17 countries. They were studying in a variety of areas, including social sciences, humanities, natural sciences, and engineering. They had visited a median of 15 countries.

Results

Task Completion

We recorded how often users completed the tasks in each stage and each condition of the experiment. The task completion is used as a measure of how location affected participants' behavior. We defined task completion as having logged into the web service *and* completed the given task. We encoded completed tasks as 1, and uncompleted tasks as 0. For each stage we summed the

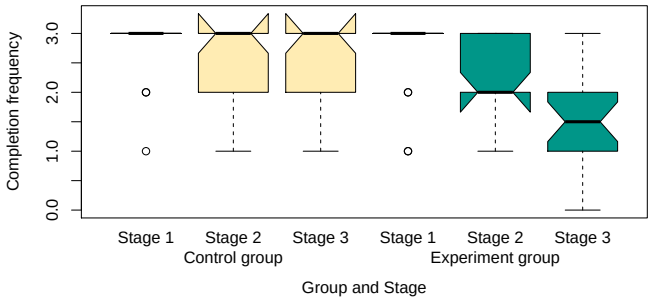


Figure 2: Box plots of task completion scores across different stages for all websites.[2]

	Control			Experiment		
Stage	Mean	Mdn	SD	Mean	Mdn	SD
1	2.82	3	0.50	2.73	3	0.63
2	2.55	3	0.60	2.32	2	0.65
3	2.32	3	0.84	1.45	2	0.96

Table 2: Descriptive statistics of task completion across different stages.

scores from the three websites to produce an aggregate score between 0 and 3.

Distributions of completion scores are shown in Figure 2. Most control group participants completed all tasks in all stages, but fewer experiment group participants completed the task when the location changed (Table 2.)

Since task completion was based on counts, we performed a between-subjects Chi-squared test on the sum of completion scores across all stages and found a significant difference between the two conditions ($\chi^2(1) = 9.44, p = 0.002$). Our post-hoc pairwise Chi-squared tests using a Bonferroni correction showed that this difference occurred in Stage 3 ($\chi^2(1) = 10.52, p = 0.011$), implying that the warning had an effect on the experiment group. We further used a Chi-squared test to look for differences between the stages in each condition. We found a significant effect of stages in the experiment group ($\chi^2(2) = 30.86, p < 0.001$), but no effect in the control group.[3] Table 3 shows the results of post-hoc pairwise Chi-squared tests. We found significant differences between Stage 1 and Stage 3, and between Stage 2 and Stage 3 for the experiment group. This showed that the warning for location changes significantly affected whether participants completed critical tasks.

Login Times

We recorded login times (in seconds) as an indicator of how much attention participants paid to the website locations. The login time was measured as the time between when the webpage loaded and when the user clicked the login button. We aggregated the times for each participant in each stage by taking the mean of the login times for the three websites. Figure 3 shows the distribution of login times across the three stages.

[2]The notches in the box plots represent the 95% confidence intervals around the median. When the intervals fall outside the 1st or 3rd quartiles, notches extend beyond the box.

[3]To conserve space, we do not report insignificant statistics.

	Control			Experiment		
Stages	χ^2	df	p	χ^2	df	p
S1 vs. S2	2.00	1	1.000	3.62	1	0.513
S1 vs. S3	6.15	1	0.118	26.15	1	< 0.001
S2 vs. S3	0.79	1	1.000	10.52	1	0.011

Table 3: Chi-squared tests of task completion across different stages using the Bonferroni correction.

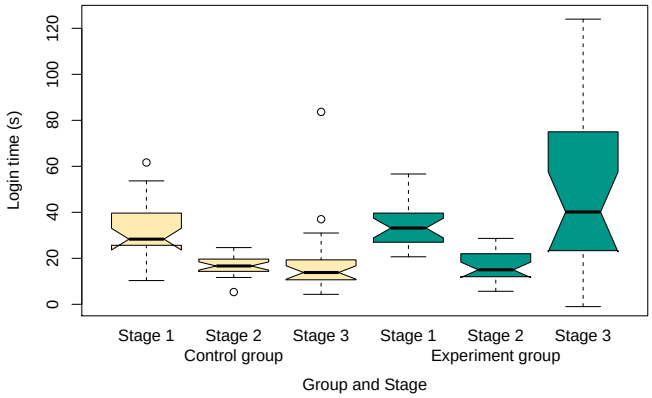


Figure 3: Box plots of time spent on website logins, averaged over all three websites in each stage.

The mean login times ranged from 16 to 54 seconds (Table 4). While the login times in Stages 1 and 2 were similar across the two groups, the times in Stage 2 were shorter. In Stage 3, the experiment group spent more time logging in.

We conducted a mixed two-way ANOVA to analyze the differences in login times between the two conditions and between the stages. There were significant effects of both condition ($F(1, 41) = 12.73, p < 0.001$) and stage ($F(2, 82) = 9.92, p < 0.001$) and a significant interaction between condition and stage ($F(2, 82) = 10.65, p < 0.001$). We then used post-hoc pairwise t-tests to observe differences between the two groups. They had significant differences only in Stage 3 ($t(21) = -3.08, p = 0.051$), implying that the warning made the experiment group spend more time than the control group. We further conducted post-hoc pairwise t-tests with a Bonferroni correction to look for differences within each group (Table 5). There were significant differences between Stages 1 and 2 for both conditions, possibly since participants became used to the login process. The experiment group had significantly different login times between Stages 2 and 3, implying that the location change warning changed their behavior.

Task Completion on Different Websites

To examine whether LocationWatch had an effect on participants' willingness to complete security-sensitive

Cond	Stg	Mean	Mdn	SD	Skew	Kurtosis
Ctrl	1	33.77	28	13.13	0.61	-0.35
	2	16.83	17	4.22	-0.59	1.44
	3	18.29	14	16.91	3.01	10.93
Expt	1	34.32	33	8.61	0.85	0.86
	2	16.64	15	6.63	0.30	-0.88
	3	54.02	41	45.12	1.11	0.77

Table 4: Descriptive statistics of login times.

	Control			Experiment		
Stages	t	df	p	t	df	p
S1 vs. S2	6.01	21	<0.001	7.24	21	<0.001
S1 vs. S3	3.52	21	0.019	-1.74	21	0.868
S2 vs. S3	-0.43	21	1.000	-3.43	21	0.023

Table 5: t-tests of login times across different stages using the Bonferroni correction.

tasks, we aggregated completion scores within the same stage in our initial task completion analysis. However, we were also interested in how users reacted to different location changes on different websites. The scale of our study prevented us from exhaustively testing different websites and locations. Nevertheless, in our study design we attempted to pick security-sensitive websites, and to choose location changes that might represent different attacks. We included location changes to countries that were neutral but implausible (Switzerland to Japan, banking), locations with well-publicized privacy issues (USA to China, Dropbox), and changes from plausible locations to other plausible locations (Sweden to USA, Facebook). As an exploratory analysis, we analyze whether there was an effect of website (and the corresponding country change) on task completion.

Using the same definition for task completion as previously, we defined a participant's task completion score for each website. The distributions of website task completion scores for the control and the experiment groups are shown in Figure 4. In both conditions, participants completed fewer tasks on Dropbox (Table 6).

A Chi-squared test using a Bonferroni correction showed a significant effect of website in both the control condition ($\chi^2(2) = 29.17, p < 0.001$) and the experiment condition ($\chi^2(2) = 32.07, p < 0.001$). Post-hoc pairwise tests showed that in both conditions, significantly fewer participants completed the tasks on Dropbox than on Facebook or banking (Table 7).

Usability

We used the System Usability Scale [10] to evaluate the usability of our location interface. Both variants of our interface were ranked as "excellent" (scores greater than 80) [35]. The average scores were 81.61 for the control group and 82.2 for the experiment group. A Mann-Whitney test found no significant difference between the two conditions.

Summary

The participants' decisions were indeed affected by their knowledge and perception of the websites' locations. In particular, there were statistically significant behavior changes in task completion when the locations changed in the experiment condition, as participants completed fewer tasks overall than before. This suggested that participants were alarmed by the location changes and some responded by avoiding performing sensitive tasks online. Participants who completed the tasks when the locations changed mainly cited the website's reputation as the main reason for them to proceed. They sometimes resorted to extra steps to validate the authenticity of the websites. For example, when the location changed, some participants tried connecting to the designated website by searching for it using multiple search engines.

LocationWatch did not interrupt users in non-critical cases since both groups had similar login times in Stages 1 and 2. Our post-hoc tests showed that there was a significant difference in Stage 3, in which warnings were shown in the experiment condition. In this stage, the experiment group had significantly higher login times, potentially because they were deciding how to proceed or looking up reference information. Together with the task completion, this showed that the tool managed to attract user attention with the warning message.

Location information may have increased significance in certain tasks which participants perceived as sensitive. In particular, significantly fewer participants completed the Dropbox tasks, citing that they would not feel comfortable uploading personal information in such situations. However, many participants still logged in despite warnings in the banking task, which was considered to be sensitive from the qualitative analysis. This may potentially be due to their impression of the country (Japan).

In addition to identifying location's role in users' decision making, our evaluation also showed that LocationWatch was usable. SUS scores were good and similar for both groups. This showed that the version with the location change warning was as usable as existing solutions which primarily show the country flag (control group). The warning was also a desired feature since similar notifications were suggested by many participants in the control group (8 out of 22) during the post-study discussion. As LocationWatch has a similar purpose to certificate validation, it may be useful to incorporate it with existing certificate indicators.

DISCUSSION AND CONCLUSION

When deciding whether to trust websites with personal information or files, users base their judgments on a variety of factors. These include the website's appearance, the company's reputation and perceived reliability, the urgency of the matter, the amount of the transaction,

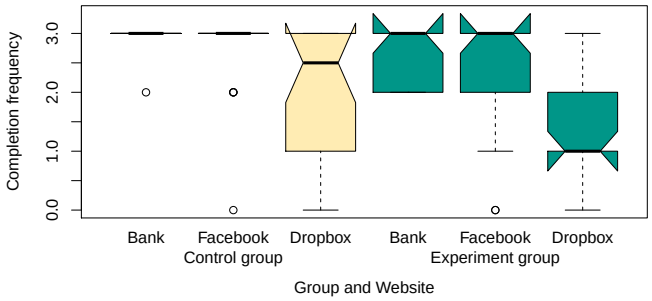


Figure 4: Box plots of the task completion scores across different websites for all stages.

	Control			Experiment		
Stage	Mean	Mdn	SD	Mean	Mdn	SD
1	2.95	3	0.21	2.64	3	0.49
2	2.95	3	0.70	2.45	3	0.96
3	2.00	3	1.15	1.14	1	0.91

Table 6: Descriptive statistics of task completion across different websites.

and the presence of danger signals such as TLS warnings. However, many of these factors are subjective and can be easily spoofed (e.g., in a phishing attack). Users need to be provided with reliable and comprehensible indicators that they can use in their trust assessments.

With the advent of verifiable protocols for location-based web authentication [1, 44], location can be used as such a factor. Our studies showed that website locations are intuitive, comprehensible, and tangible, and can be related to other issues that concern users. In our interviews, participants spoke about ways that location information could help them address concerns relating to legal/jurisdictional issues, environmental issues, and others. One of the problems with TLS certificates is that the user is only asked to handle the situations where certificate validation has failed. Web server location verification is set up in the same way, but unlike TLS certificate verification, location verification frames the problem in an approachable and interpretable way for the end user. Our study showed that when alerted to a location change, users understand the change and interpret it in the light of their current task and the perceived importance of the situation.

Of course, the judgments made by users in these situations may be affected by personal experience or cultural bias. This is unavoidable because each person's judgment is shaped by their individual experiences and perspective. In spite of this subjectivity, it is helpful to frame the problem using comprehensible information, rather than asking the user to interpret technical information (as in a TLS certificate). Participants in our study used the location changes in their evaluations with alternative strategies. These include inspecting the web page design, obscuring metadata (e.g., one participant changed the name of the file uploaded to Dropbox from `passport.pdf` to `holiday.pdf`), and deleting data from the websites after completing the tasks.

	Control			Experiment		
Tasks	χ^2	df	p	χ^2	df	p
B vs. FB	2.41	1	0.722	0.53	1	1.000
B vs. DB	21.06	1	<0.001	23.32	1	<0.001
FB vs. DB	10.20	1	0.008	15.99	1	<0.001

Table 7: Chi-squared tests of task completion across different websites using the Bonferroni correction.

The element of subjectivity also affected our study design. We conducted our user study in the lab to obtain richer data about participants' interactions with LocationWatch. This in turn limited the diversity of perspectives that we were able to capture (both in terms of participants and the number of websites and locations we could present). In future work, it would be interesting to conduct a larger scale study using crowdsourcing platforms to capture a more global perspective. Despite these limitations, our study is the first to explore how users can reason with location information and integrate it into their decision-making about security and privacy.

We expect that in the future, location verification could become an important consideration for data center deployment, which is presently concerned with infrastructure and sustainability [41]. Companies currently often contract their web hosting to content delivery networks (CDNs), which distribute data from the "origin" to servers closer to the clients (often to the same city or region). Market pressure might encourage companies to choose CDNs storing data in preferred locations. We see the beginnings of this with EV certificates [11], where a premium is paid to obtain certificates with verified company locations. Automatic and verifiable location information would increase the utility of such a system.

Authenticating websites is an important problem since it relates to users' trust in online services. The current certificate model forces users to interpret dense and unfamiliar technical information, which results in users expressing confusion about warnings or ignoring them [14]. Website location offers a complementary approach to certificate validation that is tangible, comprehensible and relatable for users. Our studies showed that users were less likely to complete security-sensitive tasks when warned about location changes. Website location indication is a usable approach to helping users make good privacy and security assessments online.

REFERENCES

1. AbdelRahman Abdou and P.C. van Oorschot. 2016. Server Location Verification and Server Location Pinning: Augmenting TLS Authentication. *arXiv preprint arXiv:1608.03939* (2016).

2. Alessandro Acquisti, Laura Brandimarte, and George Loewenstein. 2015. Privacy and human behavior in the age of information. *Science* 347, 6211 (Jan. 2015), p509–514.
3. Devdatta Akhawe and Adrienne Porter Felt. 2013. Alice in warningland: A large-scale field study of browser security warning effectiveness. In *Presented as part of the 22nd USENIX Security Symposium (USENIX Security 13)*. 257–272.
4. Hazim Almuhimedi, Adrienne Porter Felt, Robert W Reeder, and Sunny Consolvo. 2014. Your Reputation Precedes You: History, Reputation, and the Chrome Malware Warning. In *SOUPS*. 113–128.
5. Amazon Web Services. 2016. AWS Global Infrastructure. https://aws.amazon.com/about-aws/global-infrastructure/. (2016).
6. APNIC. 2016. Asia-Pacific Network Information Centre. https://www.apnic.net/. (2016).
7. ARIN. 2016. American Registry for Internet Numbers. https://www.arin.net/. (2016).
8. Louise Barkhuus and Anind K Dey. 2003. Location-Based Services for Mobile Telephony: a Study of Users' Privacy Concerns. In *INTERACT*, Vol. 3. p702–712.
9. Virginia Braun and Victoria Clarke. 2006. Using thematic analysis in psychology. *Qualitative Research in Psychology* 3, 2 (Jan. 2006), p77–101.
10. John Brooke. 1996. SUS-A quick and dirty usability scale. *Usability evaluation in industry* 189, 194 (1996), p4–7.
11. CAB Forum. 2016. EV SSL Certificate Guidelines. https://cabforum.org/extended-validation/. (2016).
12. Sunny Consolvo, Ian E Smith, Tara Matthews, Anthony LaMarca, Jason Tabert, and Pauline Powledge. 2005. Location disclosure to social relations: why, when, & what people want to share. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, p81–90.
13. Dave G. 2016. Flagfox. https://flagfox.net/. (2016).
14. Adrienne Porter Felt, Alex Ainslie, Robert W Reeder, Sunny Consolvo, Somas Thyagaraja, Alan Bettes, Helen Harris, and Jeff Grimes. 2015. Improving SSL warnings: comprehension and adherence. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems (CHI)*. ACM, p2893–2902.
15. Adrienne Porter Felt, Robert W Reeder, Alex Ainslie, Helen Harris, Max Walker, Christopher Thompson, Mustafa Embre Acer, Elisabeth Morant, and Sunny Consolvo. 2016. Rethinking Connection Security Indicators. In *Twelfth Symposium on Usable Privacy and Security (SOUPS)*.
16. Adrienne Porter Felt, Robert W Reeder, Hazim Almuhimedi, and Sunny Consolvo. 2014. Experimenting at scale with google chrome's SSL warning. In *Proceedings of the 32nd annual ACM conference on Human factors in computing systems*. ACM, 2667–2670.
17. Drew Fisher, Leah Dorner, and David Wagner. 2012. Short paper: Location privacy: User behavior in the field. In *Proceedings of the Second ACM Workshop on Security and Privacy in Smartphones and Mobile Devices*. ACM, p51–56.
18. B J Fogg, Preeti Swani, Marissa Treinen, Jonathan Marshall, Othman Laraki, Alex Osipovich, Chris Varma, Nicholas Fang, Jyoti Paul, Akshay Rangnekar, and John Shon. 2001. What makes Web sites credible?. In *Proceedings of the International Conference on Human Factors in Computing Systems (CHI)*. ACM, p61–68.
19. Geobytes. 2016. Geobytes IP Address Locator. http://geobytes.com/iplocator/. (2016).
20. Google. 2016a. Google Data Center Locations. http://www.google.com/about/datacenters/inside/locations/index.html. (2016).
21. Google. 2016b. Google for Work Security and Compliance Whitepaper. https://static.googleusercontent.com/media/www.google.com/en/US/work/apps/business/files/google-apps-security-and-compliance-whitepaper.pdf. (2016).
22. Jefferson B Hardee, Ryan West, and Christopher B Mayhorn. 2006. To download or not to download: An Examination of Computer Security Decision Making. *ACM SIGCSE Bulletin* 13, 3 (May 2006), 32–37.
23. Giovanni Iachello, Ian Smith, Sunny Consolvo, Mike Chen, and Gregory D Abowd. 2005. Developing privacy guidelines for social location disclosure applications and services. In *Proceedings of the 2005 Symposium on Usable Privacy and Security (SOUPS)*. ACM, p65–76.
24. Iulia Ion, Niharika Sachdeva, Ponnurangam Kumaraguru, and Srdjan Čapkun. 2011. Home is safer than the cloud!: privacy concerns for consumer cloud storage. In *Proceedings of the Seventh Symposium on Usable Privacy and Security (SOUPS)*. ACM.
25. IP2Location.com. 2016. IP2Location. http://www.ip2location.com/. (2016).
26. IPligence. 2016. IPligence Geolocation Solutions. http://www.ipligence.com/. (2016).
27. ISO 9241:210 2010. *Ergonomics of human-system interaction – Part 210: Human-centred design for interactive systems*. Standard. International Organization for Standardization.

28. Ruogu Kang, Laura Dabbish, Nathaniel Fruchter, and Sara Kiesler. 2015. “My Data Just Goes Everywhere:" User Mental Models of the Internet and Implications for Privacy and Security. In *Eleventh Symposium On Usable Privacy and Security (SOUPS)*. p39–52.
29. Robert S Laufer and Maxine Wolfe. 1977. Privacy as a Concept and a Social Issue: A Multidimensional Developmental Theory. *Journal of Social Issues* 33, 3 (1977).
30. MaxMind. 2016. IP Geolocation and Online Fraud Prevention | MaxMind. https://www.maxmind.com/. (2016).
31. myip.ms. 2016. IP Whois and Flags Chrome and Websites Rating. http://chrome.myip.ms/. (2016).
32. Sameer Patil, Gregory Norcie, Apu Kapadia, and Adam J Lee. 2012. Reasons, rewards, regrets: privacy considerations in location sharing as an interactive practice. In *Proceedings of the 5th Symposium on Usable Privacy and Security*.
33. Penton. 2016. Data Center Knowledge. http://www.datacenterknowledge.com/. (2016).
34. RIPE. 2016. Regional Internet Registry for Europe, the Middle East and parts of Central Asia. https://www.ripe.net/. (2016).
35. Scott Ruoti and Kent Seamons. 2016. Standard Metrics and Scenarios for Usable Authentication. In *Symposium on Usable Privacy and Security (SOUPS)*.
36. Dongwan Shin and Rodrigo Lopes. 2011. An empirical study of visual security cues to prevent the SSLstripping attack. In *Proceedings of the 27th Annual Computer Security Applications Conference*. ACM, 287–296.
37. Jennifer Sobey, Robert Biddle, Paul C van Oorschot, and Andrew S Patrick. 2008. Exploring user reactions to new browser cues for extended validation certificates. In *European Symposium on Research in Computer Security*. Springer, 411–427.
38. Andreas Sotirakopoulos, Kirstie Hawkey, and Konstantin Beznosov. 2011. On the challenges in usable security lab studies: lessons learned from replicating a study on SSL warnings. In *Proceedings of the Seventh Symposium on Usable Privacy and Security*. ACM, 3.
39. Joshua Sunshine, Serge Egelman, Hazim Almuhimedi, Neha Atri, and Lorrie Faith Cranor. 2009. Crying Wolf: An Empirical Study of SSL Warning Effectiveness. In *USENIX Security Symposium*. 399–416.
40. USA Today. 2012. Top secret Visa data center banks on security, even has moat. http://usatoday30.usatoday.com/tech/news/story/2012-03-25/visa-data-center/53774904/1. (2012).
41. Verne Global. 2013. Data Centre Risk Index. https://verneglobal.com/media/data-centre-risk-index-2013.pdf. (2013).
42. Ryan West. 2008. The Psychology of Security. *Communications of the ACM* 51, 4 (April 2008), p34–40.
43. Alma Whitten and J Doug Tygar. 1999. Why Johnny Can’t Encrypt: A Usability Evaluation of PGP 5.0.. In *Usenix Security*, Vol. 1999.
44. Der-Yeuan Yu, Aanjhan Ranganathan, Ramya Jayaram Masti, Claudio Soriente, and Srdjan Capkun. 2016. SALVE: Server Authentication with Location VErification. In *Proceedings of the 22nd Annual International Conference on Mobile Computing and Networking (MobiCom)*.